

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A method for preventing ~~an illegal~~ use of a mobile communication terminal comprising ~~the steps of:~~

transmitting a short message service (SMS) message to ~~a lost~~ the mobile communication terminal when a user requests a phone-locking service, wherein a general SMS message processing is performed if the SMS message has no ciphered string; and

analyzing the received SMS message to set a phone-locking state for the ~~lost~~ mobile communication terminal.

2. (Original) The method of claim 1, wherein the SMS message includes a header and a ciphered string.

3. (Currently Amended) The method of claim 1, wherein the phone-locking function ~~setting step~~ comprises:

checking whether a ciphered string is contained in the received SMS message;

discriminating a type of the ciphered string; and

setting the ~~lost~~ mobile communication terminal to a phone-locking state, if the ciphered string is for a phone-locking ~~use~~ state.

4. (Currently Amended) The method of claim 3, wherein the phone-locking state setting step comprises:

reading a lock code from a memory;

enabling a variable value for the phone-locking state; and

setting the phone-locking state on the basis of the read lock code and displaying

[[a]] the phone-locking state on an LCD screen the mobile communication terminal.

5. (Currently Amended) A method for preventing ~~an illegal~~ use of a mobile communication terminal comprising ~~the steps of~~:

transmitting an SMS message to ~~a lost~~ the mobile communication terminal from an exchange when a phone-locking service is requested; and

analyzing the received SMS message and turning off an LCD power by the ~~lost~~ mobile communication terminal.

6. (Original) The method of claim 5, wherein the SMS message includes a header and a ciphered string.

7. (Currently Amended) The method of claim 5, wherein the LCD power turning off step comprises:

checking whether a ciphered string exists in the SMS message;

discriminating a type of the ciphered string contained in the SMS message; and  
turning off the LCD power, if the type of the ciphered string is for an LCD power  
[[OFF]] off use.

8. (Currently Amended) A method for preventing ~~an illegal~~ use of a mobile communication terminal comprising:

a first step in which when a user requests a phone-locking service, an SMS message is transmitted to the ~~lost~~ mobile communication terminal; and

a second step in which the received SMS message is analyzed to set a phone-locking lock function or ~~turn-off~~ an LCD power off function by controlling a general purpose input/output (GPIO) port of a mobile station modem (MSM) and cutting off power to the LCD.

9. (Original) The method of claim 8, wherein the SMS message includes a header and a ciphered string.

10. (Currently Amended) The method of claim 8, where the second step comprises:  
checking whether a ciphered string is contained in the SMS message;  
discriminating a type of the ciphered string contained in the SMS message; and

setting a ~~phone-locking~~ phone-lock function or ~~turning off the~~ LCD power off function according to the discriminated ciphered string type.

11. (Currently Amended) The method of claim 10, wherein the ~~phone-locking state~~ phone-lock function setting step comprises:

reading a lock code if the ciphered string is for a ~~phone-locking use~~ phone-lock function;

enabling a variable value for a ~~phone-locking~~ the phone-lock function; and  
setting a ~~phone-locking state~~ the phone-lock function based on the basis of the read lock code and displaying a ~~phone-locking state~~ the phone-lock function on the LCD screen mobile communication terminal.

12. (Currently Amended) The method of claim 10, wherein the LCD power ~~turning off step~~ function setting comprises[[:] ]

~~controlling a general purpose input/output (GPIO) port of a mobile station~~  
~~modem (MSM) and cutting off power applied to the LCD; and~~  
converting a data variable of a memory.

13. (Original) The method of claim 10, wherein, if no ciphered string is contained in the SMS message, a general SMS message processing is performed.

14. (Currently Amended) A method for preventing ~~an illegal~~ use of a mobile communication terminal comprising ~~the steps of~~:

receiving an SMS message from a base station;

checking whether a ciphered string exists in the received SMS message;

discriminating a type of the ciphered string if a ciphered string exists in the SMS message, and processing a general SMS message if a ciphered string does not exist in the received SMS message; and

setting a phone-locking state or turning off an LCD power off state for the ~~lost~~ mobile communication terminal according to the discriminated ciphered string type.

15. (Currently Amended) The method of claim 14, wherein the received SMS message includes a header and a ciphered string.

16. (Currently Amended) The method of claim 14, wherein the phone-locking state setting ~~step~~ comprises:

reading a lock code from the memory if ~~[[the]]~~ a ciphered string is for ~~[[a]]~~ the phone-locking ~~[[use]]~~ state;

enabling a variable value for the phone-locking state; and

setting the phone-locking state on the basis of the read lock code and displaying the phone-locking state on the ~~LCD screen~~ mobile communication terminal.

17. (Currently Amended) The method of claim 14, wherein the LCD power ~~turning~~  
off ~~step~~ state setting comprises:

controlling ~~[[the]]~~ a GPIO port of ~~[[the]]~~ an MSM and cutting off power applied  
to the LCD; and

converting a data variable of ~~[[the]]~~ a memory as the applied power is cut off.

18. (Cancelled)

19. (New) An apparatus for preventing use of a mobile communication terminal,  
comprising:

receiving means for receiving an SMS message from a base station;

checking means for checking whether a ciphered string exists in a received SMS  
message;

discriminating means for discriminating a type of the ciphered string if a ciphered  
string exists in the SMS message, and processing a general SMS message if a ciphered string does  
not exist in the received SMS message; and

setting means for setting a phone-locking state or an LCD power off state for the  
mobile communication terminal according to the discriminated ciphered string type.

Serial No. 09/987,099

Docket No.P-0287

Amtd. Dated August 19, 2004

Reply to Office Action of May 21, 2004

20. (New) The apparatus of claim 19, wherein the received message includes a ciphered string.

21. (New) The apparatus of claim 19, wherein the setting means includes control means for controlling a GPIO port of an MSM.